Public-key cryptography, (also known as asymmetric cryptography), is a form of cryptography in which a user has a pair of cryptographic keys - a *public key* and a *private key*. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

The basis for the use of the term "split key" (i.e., public key/private key procedures) is found inherently in the specification in terms of its description of the invention. (See specification page 6, lines 20 – 32) The typical SSL Certificate consists of a public key and a private key. In the present invention, the public key is used to encrypt information and the private key is used to decipher it.

For example, when a Web browser points to a secured domain, a Secure Sockets Layer (SSL) handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key

Every SSL Certificate is created for a particular server in a specific domain for a verified business entity. The SSL Certificate is issued by a trusted authority, the Certificate Authority. When the SSL handshake occurs, the browser requires authentication from the server. A customer sees the organization name when they click certain SSL trust marks or use a browser that supports Extended Validation. If the information does not match or the certificate has expired, the browser displays an error message or warning.

The description of how the invention functions supports the use of the "split key language as there is a public and private key described.

The Examiner's rejection of the claims under 35 USC § 112, first paragraph is incomplete as he has not provided the proper foundation for the rejection. The rejection of claim 1 et seq., is based upon assertions by the Examiner as to the content of the prior art. 37 C.F.R. 1.104(d)(2) states "...When a rejection in an application is based on facts within the personal knowledge of an employee of the Office, the data shall be as specific as possible, and the reference must be supported, when called for by the applicant, by the affidavit of such employee, and such affidavit shall be subject to contradiction or explanation by the affidavits of the applicant and other persons..."

Applicants submit that the Examiner should comply with the excerpt of 37 CFR 104 cited above and provide the required information relating to the supported basis for the rejection.

The Examiner is respectfully requested to reconsider his rejection of claims 1 - 4, 10 and 11 under 35 U.S.C. §102(e) as being anticipated by United States Patent 5,932,902 to Clark.

The Examiner is respectfully requested to review his interpretation of the Clark reference and the manner in which he has applied same to the claims in the instant application. By virtue of the nature of the rejection under 35 U.S.C. § 102(e), the Examiner is asserting that each and every element claimed by Applicants is found in the Clark reference. The Examiner in his rejections in the above-noted Office Action cites the specific language found in Applicants' claims and bases his anticipation rejections on excerpts which, in fact, do not support his assertions and are taken out of context.

The Examiner's rejections are quoted *verbatim* and listed *seriatem,* with Applicants' responses to the specific rejection presented immediately thereafter.

The Examiner says: "As to claim 1, Clark discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:
the devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [Column 4, lines 30 – 53]..."

Response: Applicants respectfully submit that Clark does not disclose the variety of devices that are claimed by Applicants. Clark states at Column 3, lines 1 – 3: "...the present invention relates to a system and method for securely linking computers using an intelligent token. There is no mention of the other devices. In reviewing this cited text, there is no mention of the other devices claimed, and there is no teaching nor suggestion that the RF signals are used for any purpose. A reading of the entire specification confirms that the Clark invention is restricted to operating solely between computers. Consequently there is no proper basis upon which to expand the teaching.

Clark discloses a system that uses a "Smart Card." This "Smart Card" is different from the Smart Card used in accordance with Applicants' invention.

Clark states at Column 3, lines 49 – 62:

In a preferred embodiment, the intelligent token 10 may be a smart card marketed under the trade designation MCOS32k by Gemplus International. The International Standards Organization (ISO) defines a smart card as a credit card sized piece of plastic having an embedded IC. While the MCOS32k is particularly preferred, several chip vendors including SGS Thompson, Datakey and Toshiba provide IC's for use with intelligent tokens in the form of smart cards, keys and PCMCIA cards that may be used with the instant invention. In general, these vendors have employed micro-controllers in their IC's with clock rates much lower than typical desktop computers. These IC's are used in smart cards and other intelligent tokens. However, higher performance chips are under development."

Applicants use the higher performance chips in their invention.

The inherent manner in which the Clark card operates renders it unsuitable for considering same in accordance with the present invention.

The present invention is used by a particular software application on the system to verify access authorization. This could be a single software application, which evaluates the security token and is running on top of the used hardware. Applicants detail the usage of the token to provide specific configuration information, which defines constraints for the usage of a particular user. This "constraint" e.g. temporary deactivation, limits the usage of a reduced feature set. This is more than just "authentication". It adds "authorization" patterns. The support for this is disclosure is found at page 15, the last full paragraph

"A company telephone system consists of 20 telephones hierarchically grouped into three levels, with corresponding scopes of functions. The telephone sets themselves are produced uniformly and are assigned their actual features only by means of the configuration procedure, which enables or disables various logic components in the sets depending on the customer's specific requirements."

The rejection continues:

"...the authentication comprising temporary deactivation which adds authorization patterns prior to operation [Column 6, lines 37 – 53].

Response:

Column 6, lines 37 – 53 of Clark states:

"...In keeping with the present invention, the intelligent tokens may be configured and issued by a security officer. The configuration entails loading critical information onto the intelligent token 10 including boot sector information 22 as well as digital signatures for boot files stored on the local host computer 30. At the time of issue, it is necessary to specify the machine or set of machines that the user to whom the intelligent token 10 is being issued will be granted access so that host and remote keys may be loaded. File integrity information and portions of the host operating system are also loaded onto the intelligent token 10 at this time. All data is read protected by the user's authentication information. That is, the data cannot be read unless the user password is presented correctly. The data is write protected by the security officer authentication. This arrangement prevents users from inadvertently or deliberately corrupting critical data on the intelligent token 10.."

There is no "deactivation step referred to by Clark. Applicants are deactivating the system to add authorization patterns prior to operation. (Emphasis added).

The rejection continues:

"establishment of a non-split key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, the encryption data being stored solely in the authentication system, the link between the authentication system and the device being via wired or wireless means..." [Column 6. lines 24 - 36].

Response: Applicants are not sure of the relevance of the cited excerpt with respect to the instant invention.

Clark states at Column 6, lines 24 - 36:

"As discussed above, the intelligent token 10 stores critical information such as digital file signatures for system executables and the user's cryptographic keys. Comparing executable computer file signatures of the remote and local hosts with those stored on the intelligent token 10 provides a virus detection mechanism which is difficult to defeat. This approach is consistent with recent trend to validate the file integrity rather than solely scan for known virus signatures. In addition, by authenticating both the local host computer 30 and the remote host computer 52, the intelligent token 10 may be employed to facilitate "encrypted communication" between the local host computer 30 and the remote host computer 52."

There is no reference in the excerpt cited that anticipates the element of the claim cited by the Examiner. Clark is setting up a connection between computers, but he is using a completely different security system to do so. In Applicants' invention, a key may be present on the device and the same key on the smart card, so a challenge/response can be used to authenticate the smart card. Further Applicants positively recite that they use a *"non-split key"* in the claims.

The rejection continues:

"checking the encryption data in the authentication system prior to operation of the electronic device control [Column 6 lines 24 – 36];

Because there is no definitive disclosure in the reference, one must infer from Clark, that there is only one level of authentication (access yes/no). In Applicants' invention, there is no need to transfer the credentials to the host. In particular it is preferable to keep the credentials on the smart card.

The rejection continues:

"assignment of a plurality of predetermined means of access to the electronic device control associated with the authentication system the predetermined means providing access to the physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, the software function evaluates a security token and is running on top of the physical hardware [Column 5, lines 15 - 58];"

Response: In the Clark patent, when considering *"access,"* there is only a single level of access. An important distinguishing key to the present invention is that there are different levels of access to differentiate the different levels of authentication or authorization that persons with different roles may need. The Examiner is referred to page 6 of the instant specification. The different levels are mentioned on page 6. At that location, there is a disclosure of the system being open to progressive hierarchies of access rights to the device, for example, by the production of a Master Smartcard which can be issued to customers' service personnel in order to configure large numbers of individual devices.

Further, on page 6: "Applying the method in accordance with the invention, and based on the stipulation that a single SmartCard is to be able to configure any number of devices but ' that only a Master SmartCard or a personal SmartCard can be used to shut down and/or startup/restart the devices, a device manufacturer may do the following..' ."

Applicants have differentiated between a single (standard) smart card as in Clark and their invention. The different levels are mentioned in the portion of Claim 1 that reads: "...assignment of a plurality of predetermined means of access to the device associated with the authentication system." Applicants' Claim 1 states: *"said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system."*

The final portion of the rejection of Claim 1 states:

"enabling of the means for access predetermined for the authentication system dependent on the result of the check. [Column 5, lines 15 - 38]."

Response: Applicants cannot locate any teaching or disclosure related to a multi-level security system in Column 2, line 30 to Column 3 line 7, quoted by the Examiner. Clark refers to only one level of security. There is no differentiation as to authentication based on the role of the user.

Claim 1 reads, in pertinent part: "... *establishment of a non split-key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system ...*

As to Claim 11, the Examiner has rejected the elements as set forth in Claim 1, and the responses set forth above are incorporated by reference herein for those elements. The Examiner then continues the rejection with the following:

"the method providing means of no access or full access and allow
more finely defined levels of access as defined in a user
profile for configuration or maintenance work [Column 2, line 59 to Column 3, line 7]."

Response: Applicants cannot locate any teaching or disclosure related to "no access or full access and allow more finely defined levels of access" as defined in a user profile for configuration or maintenance work at the location cited in Clark.

Applicants respectfully submit that the rejection of Claim 1 based upon "anticipation" by the Clark reference is without proper foundation. The Examiner has misinterpreted the teachings of Clark; and based upon this improper interpretation, there is no predicate for the rejection. Each and every element defined in Claim 1 is not found in the Clark reference. Thus the rejections of the dependent claims are also improper and incorrect.

The Examiner continues:

"As to Claim 2, Clark discloses that the basic means of access of functions of the device comprise at least one of the following means: disable operation of the devices, enable operation of the devices, or enable configuration of device. [Column 5, lines 63 - 67]."

Response: There is no mention of enabling the basic means of access to functions using the means claimed allegedly present in Clark at Column 5, lines 63 – 67. Clark discloses at Column 5, lines 63 – 67:

If the file integrity information is valid or the error is not considered severe then the boot sector that was loaded from the intelligent token 10 in step 76 is executed in step 86. At this point, the boot process will continue as if the boot sector had been loaded from a disk, as is traditionally the case. There is no anticipation of the elements defined in Claim 2 as disclosed in the excerpt cited by the Examiner..

The Examiner continues:

"As to claim 3, Clark discloses that the link is made without need for intermediate software layers. Column 5, lines 40 to 47."

Response: There is no mention that the link is made without the need for an intermediate

software layer in Clark . The cited location discloses:

"Because of the limited size of the memory on smart cards today, it is not yet possible to store all the information in files for an OS the size of e.g., MS/DOS on a smart card. Therefore, the other files will have to be read from a disk or other storage device. It is, however, still possible to ensure their integrity by use of integrity information, e.g., checksums for the files, stored on the intelligent token 10 (by a system administrator).

This disclosure does not state how the link is set up.

The Examiner continues:

"As to claim 4, Clark discloses in addition, the step of reading at least one of the following features embodied within the authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic. [Column 6, lines 24 - 36]."

Response: There is no mention of the features claimed in Claim 1 and in Claim 4. In the excerpt cited by the Examiner set forth above, Clark does not disclose nor anticipate the elements defined in Claim 4.

The Examiner continues:

"As to claim 10, Clark discloses program code areas for the execution or preparation for execution of the steps when the program is installed in a computer. [Column 5, lines 40 – 47."

Response: Applicants can find no relevance in the disclosure at Column 5, lines 40 – 47 relating to the content of Claim 10 and request specific clarification as to the relevance of the cited lines in Clark to Claim 10. The excerpt refers to memory problems on smart cards due to limited size.

The Examiner continues:

"As to claim 11, Clark discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: [the balance of the claim is as defined in claim 1.

Response: With respect to responding to the rejection of Claim 11, the responses to each of the elements as set forth above are incorporated by reference herein.

The Examiner is respectfully requested to reconsider his rejection of Claims 5 – 9 under 35 U.S.C. §103(a) as being unpatentable over United States Patent 5,892,902 to Clark as applied to Claim 1, and further in view of United States Patent 6,415,144 B1 to Findikli, et al.

The rejection under Section 103 is improper as there is an unwarranted assertion that the elements of Claim 1 are all disclosed by Clark. Therefore the rejections of Claims 5 – 9 are improper.

Further there is a substantive error in this rejection. The reference to Findikli et al. issued on July 2, 2002 and hence was not available as a reference when the instant application was filed. There is well-established three-factor Court directed test for examining nonobviousness. One must:

1. examine the scope of the prior art;
2. determine the differences between the prior art and the invention under consideration; and
3. look at the level of skill an ordinary practitioner of the pertinent art has.

Prior art consists of the disclosures that were publicly available when the instant invention was made. Clearly the skilled artisan could not review the Findlikil, et al. reference on September 21, 2000 when the instant application was filed. Thus the rejection should be withdrawn.

Although the rejection is improper, Applicants will respond to the rejection. The Examiner concedes that Clark does not teach that the method disclosed therein that includes (1) configuration of the devices by authorized persons, and (2) that after successful authentication device specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication system or over a network.

With respect to the latter missing element, Applicants reiterate that neither Findikli (nor Clark) disclose the variety of devices that are claimed by Applicants.. There is no mention of devices other than computers. There is no basis upon which to expand the teaching. It is improper to expand the scope of the disclosure.

Clark essentially relates to a computer system. The Clark invention is specifically tailored to operate in a certain manner and is characterized as an improvement over the prior art in which the problems therewith are discussed in Column 1, line 1 to Column 2, line 3.

Findikli discloses a method of message management using a mobile communications device with a core and protected memories. Findikli, at Column 1, line 6 1 to Column 2, line 5 provides a general description of two over-the-air teleservices with no specific direction of how either of the systems listed is used in conjunction with a specific system. The excerpt cited by the Examiner as being relevant is merely a description of the prior art as known when the application was filed. As to tailoring the cellphones to meet the needs of the subscriber, Findikli states that the systems mentioned would not be effective if the phones had been hard-coded to prevent overwrite. The skilled artisan would not combine the two references as each is so specific as to be unique in its manner of operation leaving no room for combining with the other. The Examiner cites Findikli saying over-the-air teleservices provide radio telecommunications operators with greater flexibility in tailoring wireless devices to meet the needs of their subscribers. The real task is in the detail of explicating how the "tailoring" is done. There is no basis to extrapolate the cited excerpt to assert that is says any more than what it specifically does disclose.

The Examiner acknowledges that Clark does not teach that device specific configuration data are downloaded into the devices from the authentication system etc.

With regard to Claims 5 - 9, Findikli, et al. teach download of configuration information, in an unsecured way. There is no connection to any security system on the device. There is also no way to personalize/customize the configuration without the mobile phone being registered with a service provider, which may not always be the case for all the devices (like to a landline phone, or a washing machine). There is no basis to combine these references.

As to the rejection of Claims 5 - 9, the rejections are improper. The Examiner has only cited the basis for the rejection with respect to the Clark reference. The Examiner has not applied the Findikli reference specifically to Claims 5 – 9. He has only provided an excerpt from the disclosure relating to device specific configuration data being downloaded into the devices from the authentication system without explaining in detail the relevance of the disclosure and how it applies in combination to the Clark reference.

In order to analyze the propriety of the Examiner's rejections in this case, a review of the pertinent applicable law relating to 35 U.S.C. $-103 is warranted. The Examiner has applied the Clark and Findikli, et al. references discussed above using no specificity as to the relevance of how the Findliki reference is relevant and/or is applied to Claims 5 – 9.

The Court of Appeals for the Federal Circuit has set guidelines governing the combination of references.

These guidelines are, as stated are found in Interconnect Planning Corp. v. Feil, 774 F.2d 1 132,1143,227 USPQ, 543,551 :

> When prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than hindsight gleaned from the invention itself.

A representative case relying upon this rule of law is Uniroyal, Inc. v. Rudkin-Wiley Corn., 837 F.2d 1044,5 USPQ 2d 1434 (Fed. Cir. 1988). The district court in Uniroyal found that a combination of various features fiom a plurality of prior art references suggested the claimed invention of the patent in suit. The Federal Circuit in its decision found that the district court did not show, however, that there was any teaching or suggestion in any of the references, or in the prior art as a whole, that would lead one with ordinary skill in the art to make the combination. The Federal Circuit opined:

> Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. [837 F.2d at 1051, 5 USPQ 2d at 1438, citing *Lindemann*, 730 F.2d 1452,221 USPQ 481,488 (Fed. Cir. 1984).]

There is nothing in the references cited which would suggest the desirability of combining the Findikli reference with the Clark reference when the specific basis for citing the Findikli reference as to each of the rejected claims has not been covered in the Official Action.

The Examiner in his application of the cited references is improperly picking and choosing. The rejection is a piecemeal construction of the invention. Such piecemeal reconstruction of the prior art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. $ 103.

> The ever present question in cases within the ambit of 35 U.S.C. §103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the teachings of the prior art at the time the invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original) In re Wesslau 147 U.S.P.Q. 391,393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case, because the Examiner did in fact pick and choose so much of the Findikli, et al. reference with respect to "device specific configuration data" to support the rejection and did not cover completely or accurately in the Office Action the full scope of what these varied disclosure references fairly suggest to one skilled in the art.

Further, the Federal Circuit has stated that the Patent Office bears the burden of establishing obviousness. It held this burden can only be satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the reference.

> Obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art." In re Keller, 642 F.2d 413,425,208 USPQ 871,881 (CCPA 1981). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys., 732 F.2d at 1577,221 USPQ at 933. [837 F.2d at 1075,s USPQ 2d at 1599.1

The Court concluded its discussion of this issue by stating that teachings or references can be combined only if there is some suggestion or incentive to do so.

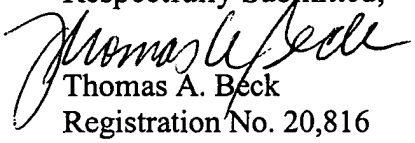
On the face of the references alone, in the present case, the skilled artisan, viewing the references would not be directed toward Applicants' system. There can reasonably be no system such as Applicants emanating from the Clark and Findikli, et al. references as the basic focus of the two references are different. There is no proper basis to combine them. Further as noted, the combination of references is improper as the Findikli et al. reference is in fact not a reference since it was not publicly available in the year 2000 when the instant application was filed.

Applicants have amended Claims 1 and 11 in this response to include additional language limitations to specifically define the invention and to clear up any ambiguities that may have existed in the wording heretofore. Further they have added Claim 12 which incorporates all of the elements of Claims 1 – 5, 8 and 9 therein. The elements of Claims 6, 7 and 10 are recited in Claims 13 – 15 respectively. Any Ccharges that may be assessed with respect to the addition of the four claims should be charge to Deposit Account 50-0510. Applicants believe that the amended claims are in a form which should result in their allowability. If there are additions to the Claims which could result in the claims being allowed, Applicants' attorney would be pleased to speak with the Examiner by phone concerning such action at a mutually agreeable time and will cooperate in any way possible.

Please address all future correspondence in this application to the undersigned at:

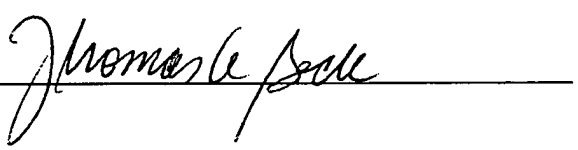
6136 West Kimberly Way, Glendale, AZ 85308-7627.

Respectfully Submitted,



Thomas A. Beck
Registration No. 20,816
6136 West Kimberly
Glendale, AZ 85308-7627
(623) 466-0080

I hereby certify that this amendment response is being transmitted by the United States Postal Service, first class mail, postage prepaid, on the date indicated below addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

Thomas A. Beck 

Date: July 8, 2007

09/667,010
DE9 19990060
09/21/2000

AMENDMENT
CHANGE OF ADDRESS